



QUALYS SECURITY CONFERENCE 2020

# Securing Cloud & Container Workloads

**Badri Raghunathan**

Director, Product Management, Qualys, Inc.

# Security Challenges in the Cloud

Lack of visibility or control on cloud resources

Misconfiguration of cloud services

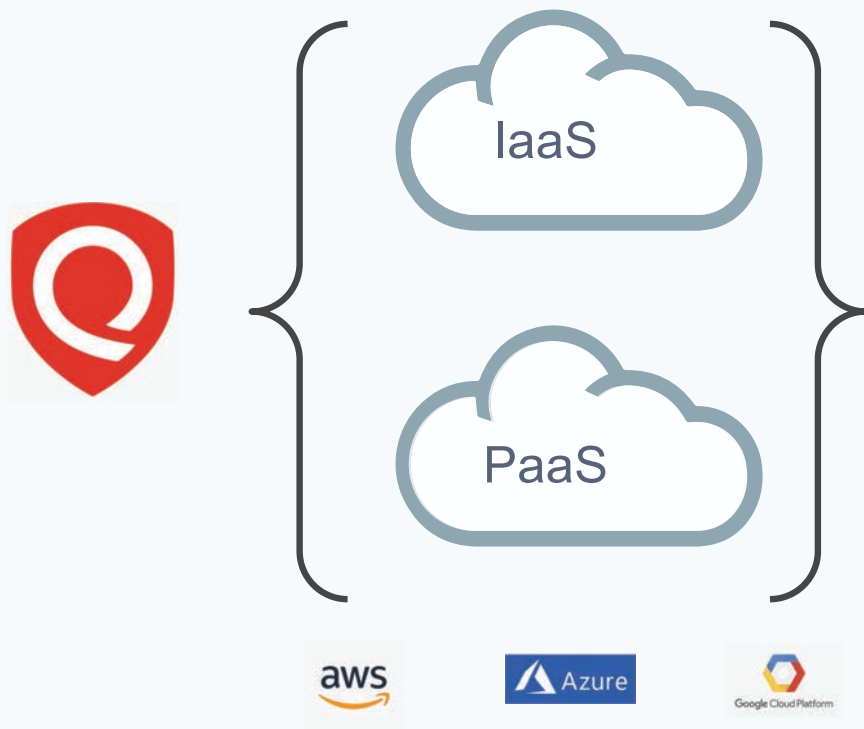
Multi cloud environment magnifies security challenges

Lack of a unified security toolset/controls for on-prem & cloud workloads

The background of the slide is a solid blue color with a subtle pattern of small white dots and faint, light blue lines radiating from the center, creating a sense of depth and connectivity. Three red circular markers are positioned on the slide: one in the upper right quadrant, one in the lower left quadrant, and one in the lower right quadrant. A semi-transparent blue rectangular box is centered on the slide, containing the text "Cloud Security" in a white, sans-serif font.

# Cloud Security

# Cloud Workload Security with Qualys



## Vulnerability Management

- Vulnerability Management (Internal & Perimeter)
- Threat Protection
- Indicators of Compromise
- Patch Management

## Policy Compliance

- Policy Compliance (incl. Secure Configuration Assessment)
- File Integrity Monitoring

## Application Security

- Web Application Scanning (WebApps and REST APIs)
- Web Application Firewall
- API Security\*

\* Upcoming feature



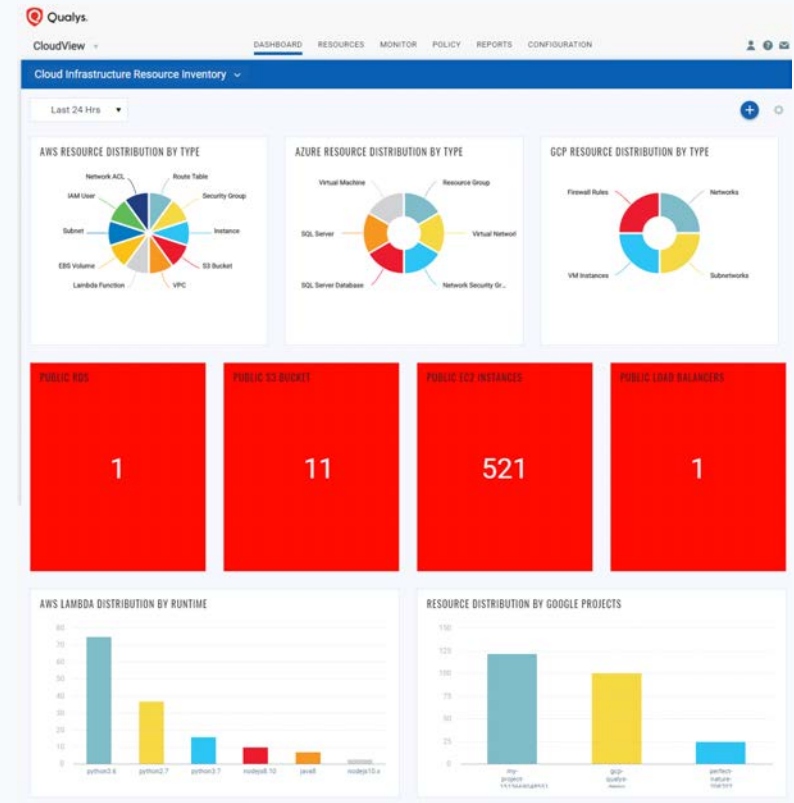
# Rich Visibility with CloudView

Visibility into your cloud resources

Identify public facing/perimeter resources

Resource usage by regions/accounts.

View associations to identify the blast radius

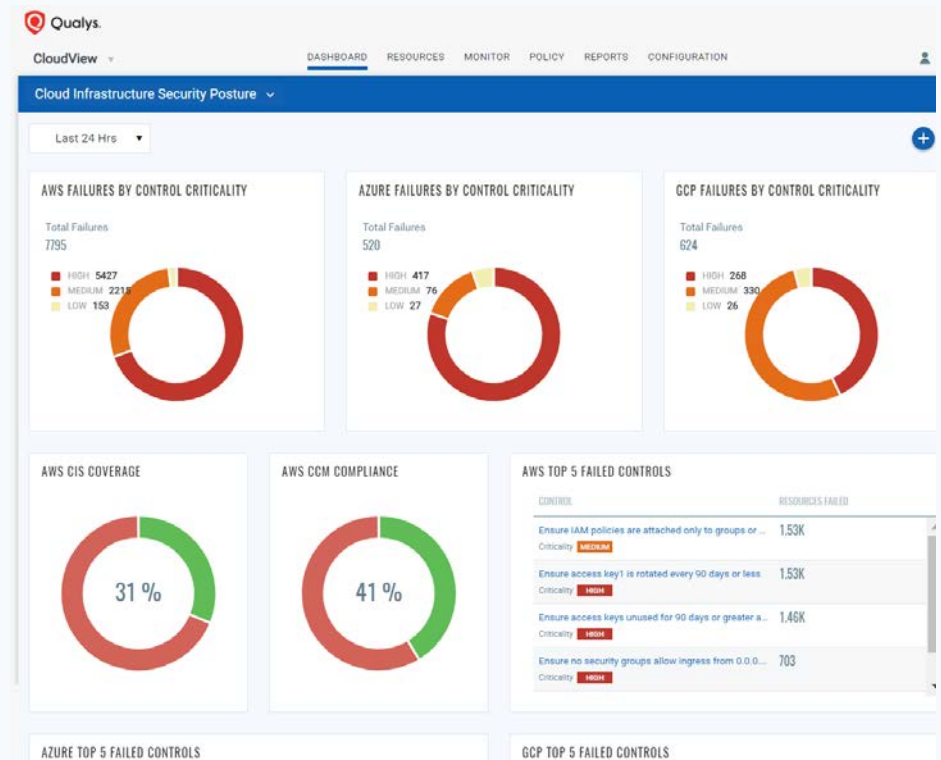


# Compliance Assessment

Identify misconfigured resources

Detect resources that are non-compliant against standards such as CIS Benchmark

Identify top failed controls/account for prioritizing the remediation efforts



# Correlate with Vulnerability Data

Identify vulnerable instances with public IP and associated with the misconfigured security groups

Use vulnerability information for cloud instances to prioritize threats better

The screenshot displays the Qualys Enterprise CloudView interface for Amazon Web Services. The top navigation bar includes links for DASHBOARD, RESOURCES, MONITOR, POLICY, REPORTS, and CONFIGURATION. The left sidebar shows a summary of 28 total instances, broken down by region: N. Virginia (16), London (7), and Mumbai (5). The main content area features a search bar with a query: `vulnerability.threatIntel.easyExploit:true and securitygroup.inboundRule.ipv4Range:0.0.0.0`. Below the search bar, there are three summary cards: 0 Without Agents, 21 With Public IP, and 2 Docker Hosts. A table titled 'Resource Summary' lists 28 instances, showing columns for EC2 Instance ID, Account ID, Region, Type, State, and First Discovered On. The table lists various instance types (t2.medium, t2.micro) and their states (Running).

EC2 Instance ID	ACCOUNT ID	REGION	TYPE	STATE	FIRST DISCOVERED ON
i-09877e1ab68f05330 demo-aws-ue1-windows-2016-public-B	636123215182	N. Virginia	t2.medium	Running	October 13, 2019 4:46 AM
i-03c8e8468ca299184 demo-aws-ew2-windows-2016-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0e8258f50a903cc4f demo-aws-ew2-ubuntu-16-public-C	636123215182	London	t2.medium	Running	October 12, 2019 8:44 PM
i-0de3c0e9cc738bcf0 demo-aws-ue1-ubuntu-16-public-B-2	636123215182	N. Virginia	t2.micro	Running	September 19, 2019 1:02 AM
i-08ad24b40b2eaf29a demo-aws-ew2-windows-2019-public-C	636123215182	London	t2.medium	Running	August 27, 2019 7:48 PM
i-0ab2ff3ca465eef42 demo-aws-ue1-centos-7-private-B	636123215182	N. Virginia	t2.medium	Running	August 27, 2019 7:48 PM
i-06f41ddd375f62144 demo-aws-mumbai-windows-2016-publi..	636122215182	Mumbai	t2.medium	Running	August 26, 2019 7:41 AM
i-0afd7b51095e0db68 demo-aws-ue1-windows-2008-public-B	636123215182	N. Virginia	t2.medium	Running	August 24, 2019 7:31 PM

NEW

# Serverless Visibility

Serverless Visibility –  
Inventory support for  
AWS Lambda functions

Best practices policy for  
identifying  
misconfigurations

**Qualys Express CloudView - Amazon Web Services**

21 Total Lambda Functions

Regions: N. Virginia (10), Ohio (7), Mumbai (2), Ireland (1), Oregon (1)

Runtime: nodejs4.3 (5), python3.7 (4), java8 (3), nodejs8.10 (3), python2.7 (3)

Tracing: PassThrough (20), Active (1)

**Qualys Express CloudView - Monitor**

11 Total Controls Evaluated

Policy: AWS Lambda Best Practices Policy

Evaluations: 1.61K (Total Evaluations), 948 (Pass), 667 (Fail), 497 (High), 48 (Medium)

CID	Control Name	Criticality	Service
97	Ensure that Lambda function has tracing enabled	High	Lambda Fun
98	Ensure that Lambda Function is not using An IAM role for more than one La...	High	Lambda Fun
99	Ensure that Multiple Triggers are not configured in Lambda Function	Medium	Lambda Fun
100	Ensure that Lambda Runtime Version is latest and not custom	Low	Lambda Fun
101	Ensure that Lambda function does not have Admin Privileges	High	Lambda Fun
102	Ensure that Lambda function does not have Cross Account Access	High	Lambda Fun



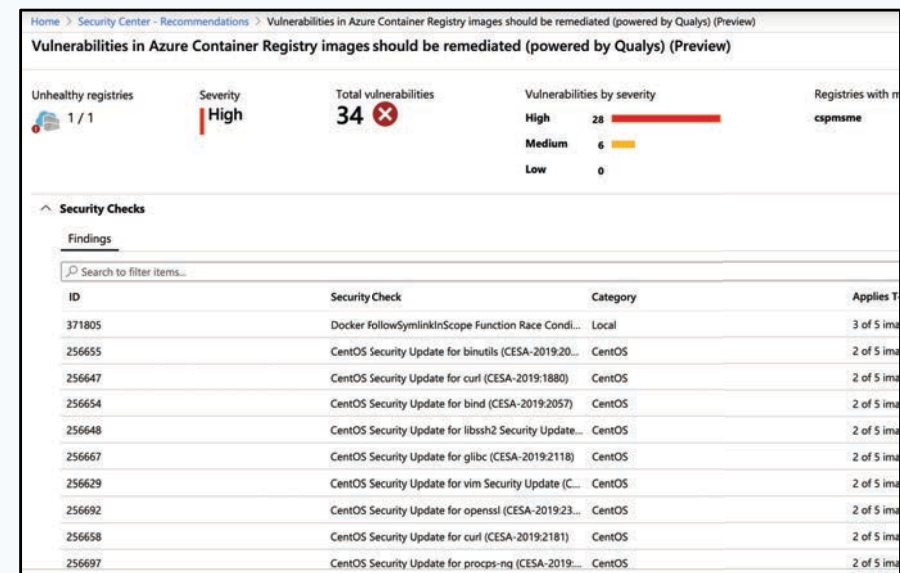
NEW

# Built-in Security with Cloud Providers

Send findings into Azure, AWS, GCP Security Hubs

Access & investigate findings from within the Cloud Provider Security console

Native integration of vulnerability assessment of hosts, containers (MSFT Azure - Powered by Qualys)



*Native Azure Host, Container Scanning (Powered by Qualys)*

The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted with a red glow, one in the upper right, one in the lower left, and one in the lower right. A semi-transparent grey rectangle is centered on the slide, containing the text "Container Security" in white.

# Container Security

NEW

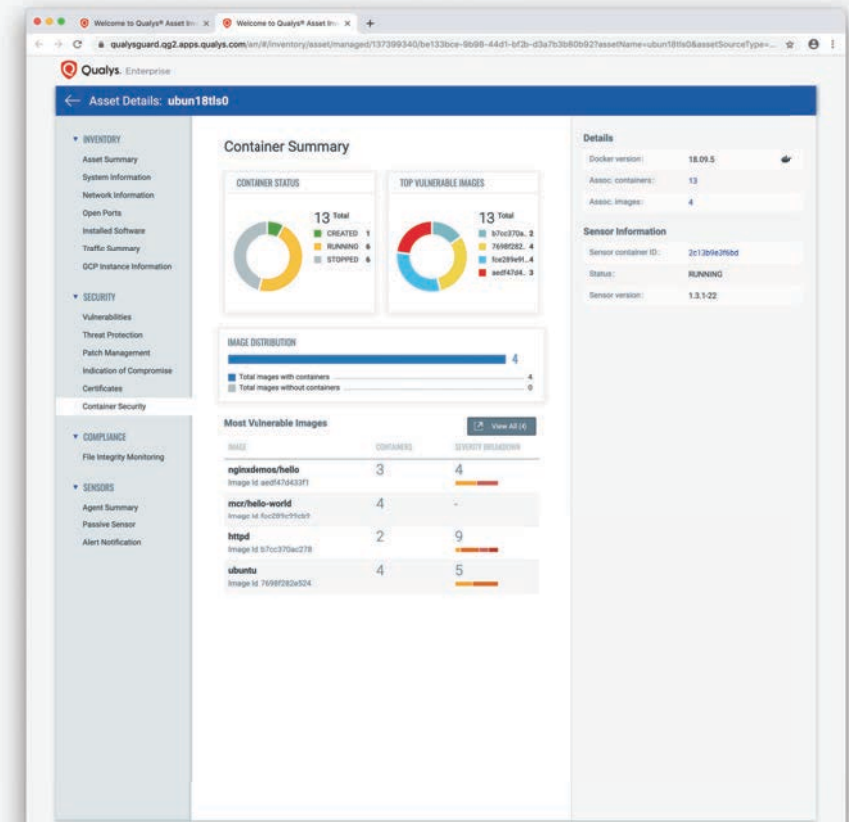
# Visibility into Container Infrastructure

Inventory for all your container infrastructure (Included with VMDBR)

Visibility into containers via Scanner, Cloud Agent, Container Sensor

Tracking DockerHub official images

Upgrade for security across DevOps pipeline



# Correlating with Vulnerability Data

Search  
based on all  
attributes

Container Security DASHBOARD ASSETS EVENTS CONFIGURATIONS India Naccount (quays\_nn)

Assets Images Containers

Search: vulnerabilities.severity:"Severity 5" and repo.registry:"docker.io"

68 Total Images

1 - 50 of 68

REGISTRY	REPOSITORY	CREATED ON	TAGS	CONTAINERS	VULNERABILITIES
docker.io	elasticsearch Image Id: 7b3c18d8f363	Feb 06, 2018	latest	0 On Hosts: 1	2
docker.io	redis Image Id: de560ba5403e	Feb 06, 2018	latest	1 On Hosts: 1	3
docker.io	kibana Image Id: 9ef680b9e227	Feb 06, 2018	latest	0 On Hosts: 1	3
docker.io	node Image Id: e606300537c6	Feb 01, 2018	latest	0 On Hosts: 1	3
docker.io	httpd Image Id: 2e202f453940	Jan 26, 2018	latest	1 On Hosts: 1	3
docker.io	cassandra Image Id: e25e005ebec1	Jan 23, 2018	latest	0 On Hosts: 1	4
docker.io	solr Image Id: 0ee0d104030e	Jan 19, 2018	latest	0 On Hosts: 2	14
docker.io	tomcat Image Id: 66bbd06c8cd	Jan 18, 2018	latest	0 On Hosts: 1	13
docker.io	kibana Image Id: 6ded4c70c32d	Jan 17, 2018	latest	0 On Hosts: 1	10

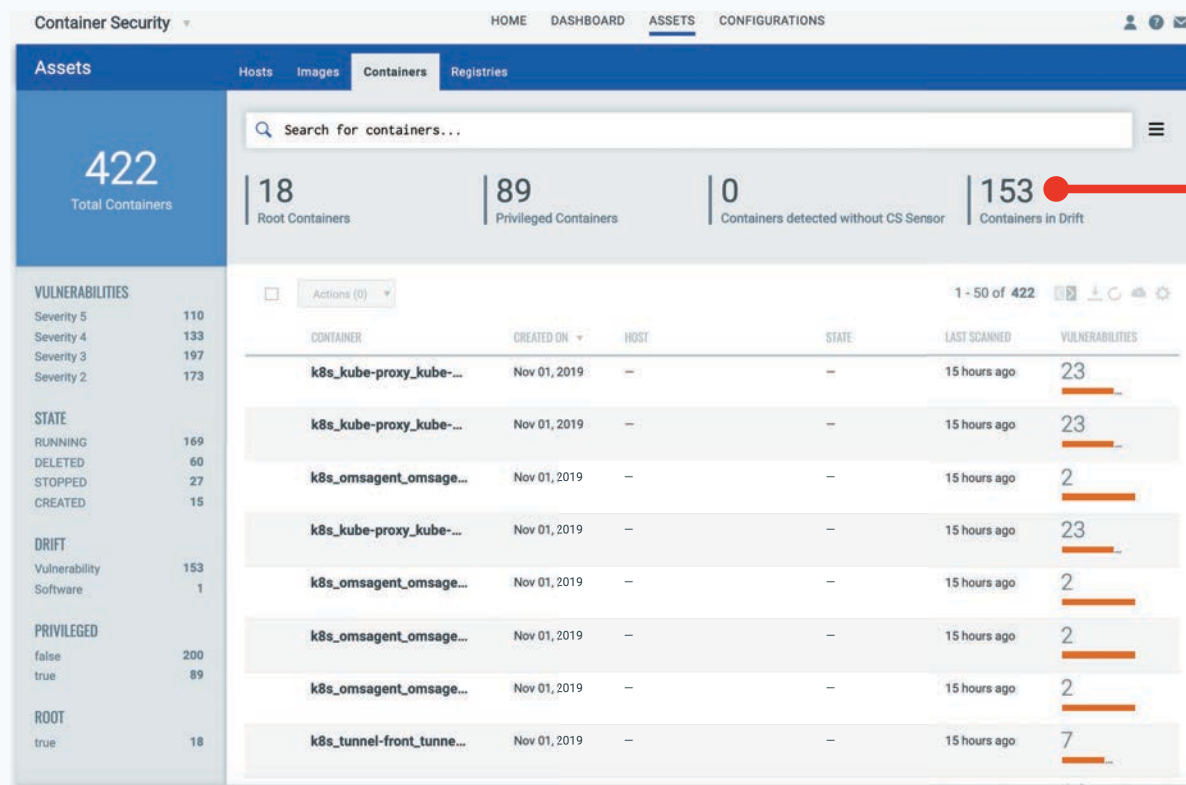
**Labels:** NGINX Docker M... 3, Http://Www.Stind... 1, GPLv2 1, /Dockerfile 1, Git 1, CentOS Base Ima... 1, Opsxcq@Strm.Sh 1, Bad-Dockerfile 1, CentOS 1, Reference Docke... 1, Https://Github.C... 1, Show less

**Registry:** Docker.io 68, Art-Hq, Intranet.Q... 1

**Vulnerabilities:** Severity 5 68, Severity 4 65, Severity 3 59

- Image info
- Registry info
- Containers for this image
- Vulnerability posture?
- Easy drill down for complete inventory

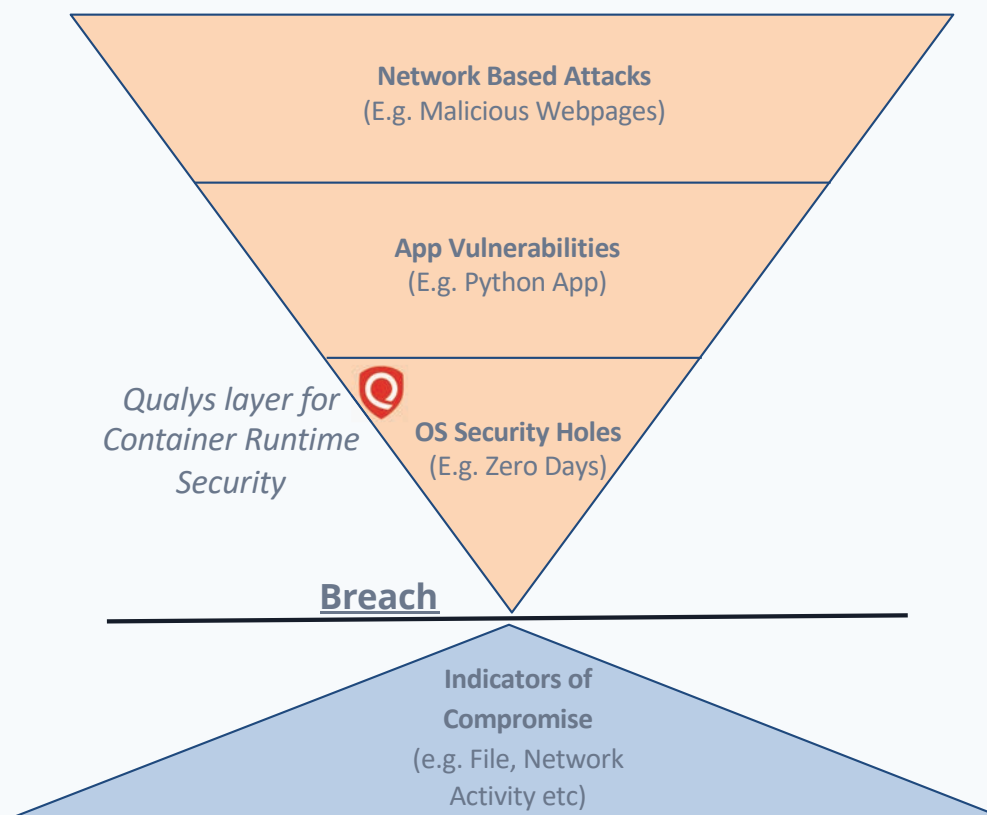
# Detecting Runtime Drift



Identify potential breaches in containers

“Drift” Containers, differ from their parent Images by vulnerability, software package composition, behavior, etc

# Detection, Response for Containers



NEW

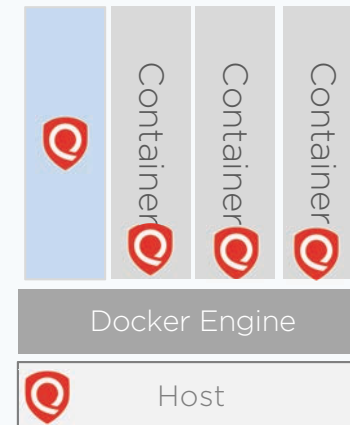
# Container Runtime Security

Integrated into Qualys Platform

Function level firewall for containers

Granular security policies to control file, network, process behavior

Built-in policies from Qualys Threat Research



← View Details: e910f86a4411

Filter by: All ▾ 1 - 50 of 63

LOG	PROCESS	PROCESS ID	CALL	ARGUMENTS	ACCESS	TIME
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libselir	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libpcr	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	2	/lib/x86_64-linux-gnu/libblik	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	0	/lib/x86_64-linux-gnu/libblik	Allowed	November 5, 2019 04:26:26AM
Behavior log	/sbin/init	1	3	/lib/x86_64-linux-gnu/libcsp	Allowed	November 5, 2019 04:26:26AM

The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted with a red glow, indicating a specific point of interest or a security alert. The word "DEMO" is centered in a white, bold, sans-serif font within a semi-transparent blue rectangular box.

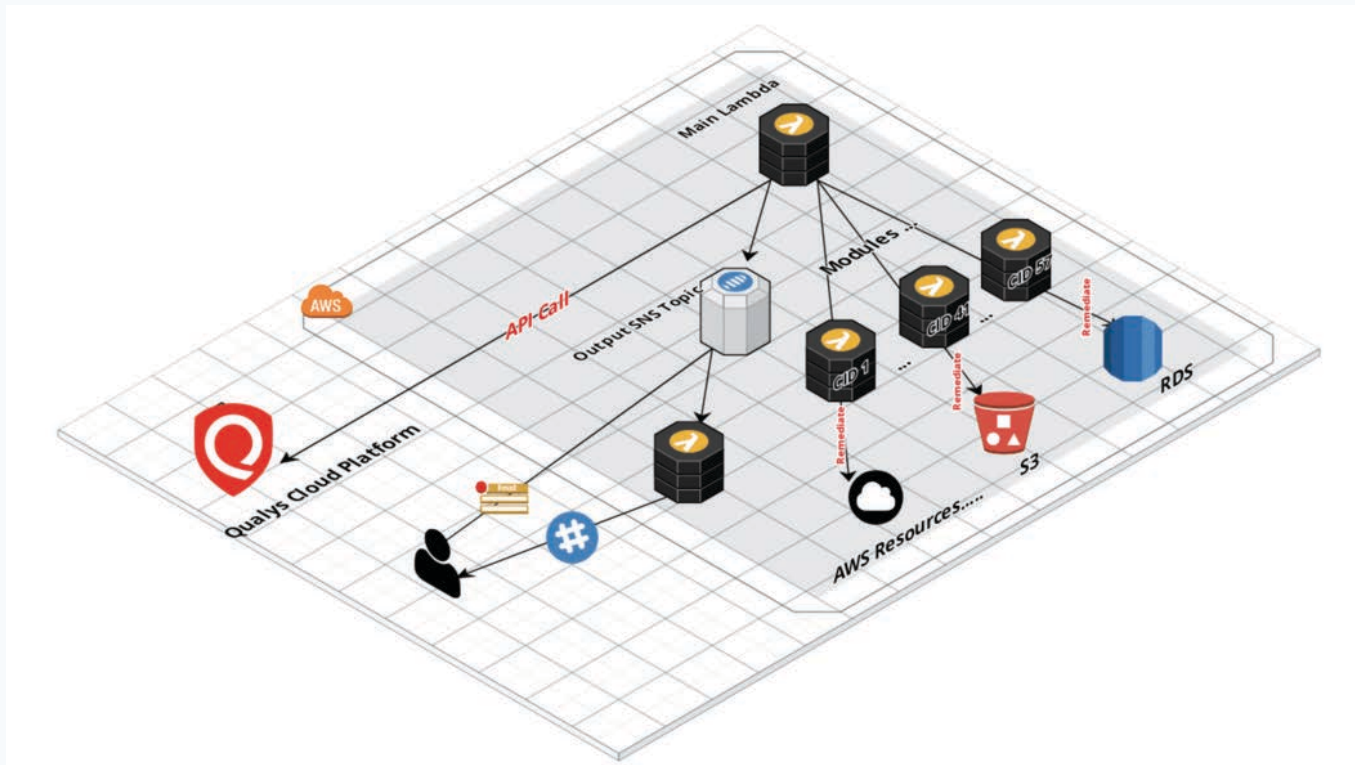
# DEMO



# The Road Ahead



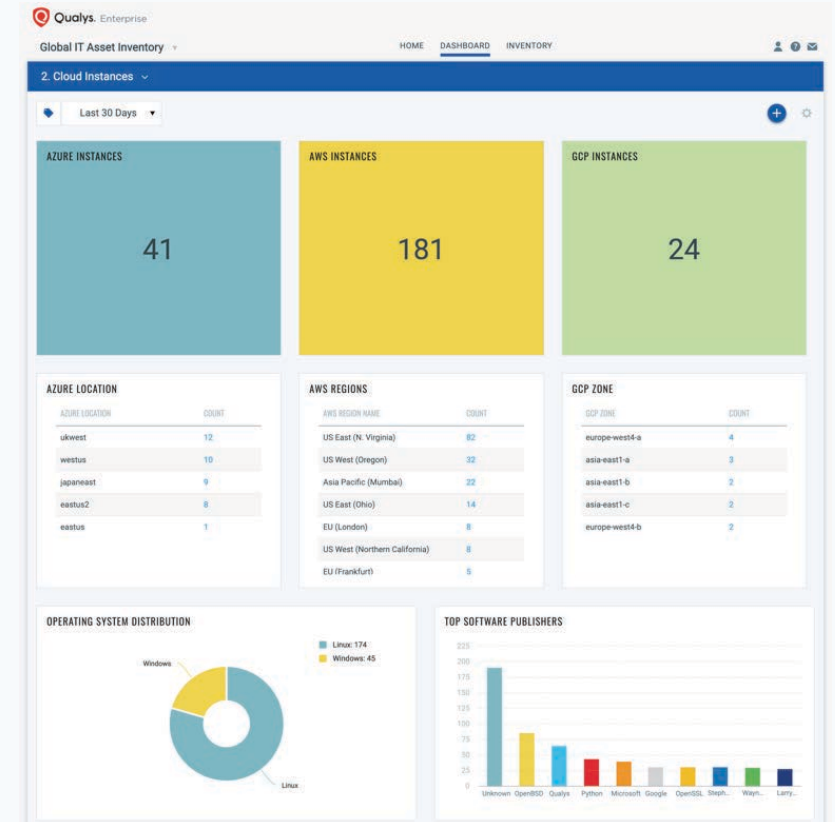
# Towards Automated Remediation



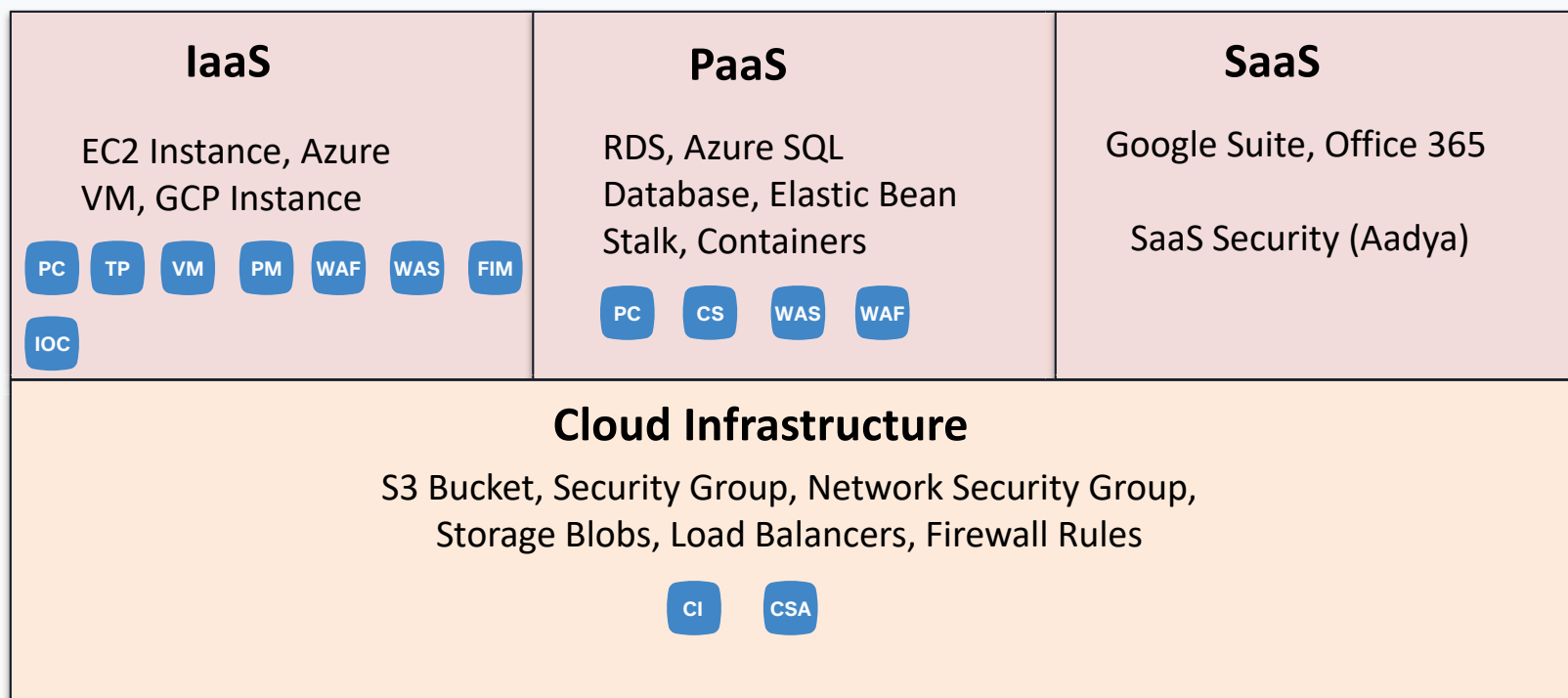
# Towards Seamless Visibility

Across application stack (Hosts, Kubernetes Pods, Containers, Serverless)

Correlate cloud inventory data with containers



# Securing Your Cloud Deployments





QUALYS SECURITY CONFERENCE 2020

# Thank You

Badri Raghunathan  
[braghunathan@qualys.com](mailto:braghunathan@qualys.com)